



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/926,594	11/23/2001	You-Jin Eun	P21705	4083
7055	7590	01/25/2006	EXAMINER	
GREENBLUM & BERNSTEIN, P.L.C.			DINH, MINH	
1950 ROLAND CLARKE PLACE			ART UNIT	
RESTON, VA 20191			PAPER NUMBER	
			2132	
DATE MAILED: 01/25/2006				

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

**Application No.**

09/926,594

**Applicant(s)**

EUN ET AL

**Examiner**

Minh Dinh

**Art Unit**

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 09 November 2005.  
2a) ☒ This action is FINAL. 2b) ☐ This action is non-final.  
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 34-66 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
6) ☒ Claim(s) 34-66 is/are rejected.  
7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.  
10) ☒ The drawing(s) filed on 23 November 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☒ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)  
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.  
4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.  
5) ☐ Notice of Informal Patent Application (PTO-152)  
6) ☐ Other: \_\_\_\_\_.

## **DETAILED ACTION**

### ***Response to Amendment***

1. This action is in response to the amendment filed 11/09/2005. Claims 1-33 have been cancelled; claims 34-66 have been added. The specification has also been amended.

### ***Response to Arguments***

2. Applicant's arguments filed 11/09/2005 have been fully considered but they are not persuasive.

Applicant argues that Reardon (6,212,635) discloses that the key pair "SG.1" is the security gateway's key pair rather than a key pair assigned to a system security manager (page 15, last paragraph). The security gateway disclosed by Reardon is a component that enforces a security policy to protect a computer system; therefore, the security gateway meets the limitation of a system security manager (Abstract; col. 3, lines 55-61). Accordingly, the key pair SG.1 is the digital signature keys of a system security manager.

In response to applicant's argument that the references fail to show certain features of applicant's invention (page 16, 1<sup>st</sup> paragraph), it is noted that the features upon which applicant relies (i.e., the security gateway does not meet the limitation of a security kernel because it is not an inner constituent of an operating system) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re*

*Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Since the security gateway implements the reference monitor concept (e.g., enforcing a security policy to protect a computer system), the security gateway meets the limitation of a security kernel.

Applicant traverses, see page 16, 2<sup>nd</sup> paragraph, the examiner's assertion of Official Notice in the previous Office Action. Reardon discloses storing the private key of the signature keys in the security kernel, but Reardon does not disclose storing the private key together with the corresponding certificate. Examiner took Official Notice that storing a private key together with the corresponding certificate is well known in the art. Accordingly, the certificate is stored together with the private key in the security kernel. Support for the Official Notice can be found in Nordenstam et al, US 6,711,263 (see figure 1; col. lines 28-46; col. 8, lines 52-64).

Applicant argues that there is not any motivation to modify Reardon (page 17, last paragraph). The motivation for combining the references was addressed in page 5 of the previous Office Action.

In response to applicant's argument that the references fail to show certain features of applicant's invention (page 18, 1<sup>st</sup> paragraph), it is noted that the features upon which applicant relies (i.e., operating in the kernel layer of the server computer operating system) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

***Claim Rejections - 35 USC § 112***

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 34-55 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- Claims 34 and 45 recite the limitation "the identifying result" in the last line. There is insufficient antecedent basis for this limitation in the claim. For examination purpose, the limitation is interpreted as "an identifying result". Claims that are not specifically addressed are rejected by virtue of their dependency.
- Claims 54-55 are method claims and yet are dependent claims of claims 47-48 which are apparatus claims.

***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2132

6. Claims 34-38, 40-49, 51-60 and 62-66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reardon (6,212,635) in view of Stein ("Web Security – A Step-by-Step Reference Guide").

Regarding claim 34 being exemplary of claims 45 and 56, Reardon disclose a method for protecting a file system in a computer, wherein a user having an access authority for a file can access the file system in the computer (Abstract; col. 8, lines 26-29), the method comprising:

generating digital signature keys and a corresponding certificate for a security gateway that enforces a security policy for a computer system and therefore, meets the limitation of a system security manager (Abstract; col. 3, lines 55-61; col. 7, lines 56-60; col. 9, line 66 – col. 10, line 59);

storing the system security manager's digital signature keys in restricted memory of a security gateway which meets the limitation of a security kernel (col. 10, lines 56-59);

generating second digital signature keys and user's certificate (col. 11, lines 10-32);

setting an access authority of the file system (col. 11, lines 10-32);

identifying a user using a PIN when the user tries to access the file system (col. 11, lines 33-44); and

giving the user the access authority for the file in accordance with identification result (col. 11, lines 33-44).

Reardon discloses storing the private key of the signature keys in the security kernel. Reardon does not disclose storing the private key together with the corresponding certificate. However, Examiner takes Official Notice that storing a private key together with the corresponding certificate is well known in the art. When a signature is generated using the private key, the corresponding certificate is sent together with the signature so that a receiving entity can use the public key from the accompanying certificate to verify the signature. It would have been obvious at the time of the invention was made to store the private key together with the corresponding certificate since storing a private key together with the corresponding certificate for ease of accessing the certificate is well known in the art. Accordingly, the certificate is stored together with the private key in the security kernel.

Reardon discloses using a password based authentication method. Reardon does not disclose using a signature based authentication method. Stein discloses using a signature based authentication method which is based on SSL (Secure Socket Layer) protocol (p. 292, Using Client Certificates for Access Control). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Reardon method to use a signature based authentication method, as taught by Stein, to overcome the vagaries of traditional password-based system.

Regarding claims 2, 13 and 24, Reardon further discloses performing a user registering/deleting process if the user is identified as the system security manager (col. 11, lines 10-32; col. 15, lines 17-28).

Regarding claims 3, 14 and 25, Reardon further discloses setting the access authority of the file system if the user is identified as the system security manager (col. 13, lines 8-37).

Regarding claims 4, 15 and 26, Reardon further discloses accessing and processing a file (col. 11, lines 27-43).

Regarding claims 5, 16 and 27, Reardon further discloses that the digital signature keys comprises a public key and a private key (col. 10, lines 54-59).

Regarding claims 7, 18 and 29, Reardon further discloses providing the user with the file system access authority to the file system if the user is the general user and providing the user with registering/deleting authority, file system access setting authority and the file system access authority (col. 11, lines 10-43; col. 15, lines 17-28).

Regarding claims 8, 19 and 30, Reardon further discloses determining whether user registration or deletion is selected; deleting data related to a user to be deleted if the user deletion is selected; and registering a user if the user registration is selected; wherein the registering step includes providing the user to be registered with the access authority; generating a secret key and a public key of the user to be registered; generating a certificate of the user to be registered; encrypting and storing the secret key of the user to be registered; and storing the certificate of the user to be registered (col. 11, lines 10-32; col. 15, lines 17-28; col. 19, lines 8-16).

Regarding claims 9, 20 and 31, Reardon further discloses that the certificate is generated by encrypting the user's public key and the access authority (col. 6, lines 9-38; col. 15, lines 24-28; col. 18, line 54 – col. 19, line 1).



Regarding claims 10, 21 and 32, Reardon further discloses selecting a file; selecting a user allowed to be access the file; and setting the access authority to the file as an access authority of the user (col. 13, lines 8-37).

Regarding claims 11, 22 and 33, Reardon further discloses receiving a name of a file to be accessed; determining whether an access authority of the file to be accessed is equal to that of the system security manager; permitting the file to be accessed if the access authority of the file to be accessed is equal to that of the system security manager; determining whether the access authority of the file to be accessed is equal to that of the user trying to access; and permitting the file to be accessed if the access authority of the file to be accessed is equal to that of the user (col. 11, lines 33-43; col. 13, lines 8-37).

7. Claims 39, 50 and 61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reardon in view of Stein as applied to claims 34, 45 and 56 above, and further in view of Abadi et al (5,315,657). As discussed in claim 1, Stein discloses using a signature based authentication method which is based on SSL (Secure Socket Layer) protocol. It is known in the art that the SSL (Secure Socket Layer) protocol authenticates a client by generating a random number at the server, sending the random number to the client, receiving the client's signature of the random number, verifying the client's certificate, extracting the client's public key from the certificate and verifying the signature to the random number. Reardon does not disclose that the manager is the certifying authority issuing the user's certificate (i.e., signing the user's

Art Unit: 2132

public key). Abadi discloses that when a new user is added to a system, the system manager issues the new user's certificate which can be verified later using the system manager's public key (col. 7, lines 27-40). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Reardon and Stein such that the manager is the certifying authority issuing the user's certificate which can be verified later using the system manager's public key, as taught by Abadi. Certificates could be generated and issued more expeditiously with an in-house certifying authority.

### ***Conclusion***

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 5,987,123 to Scott et al.

U.S. Patent No. 6,249,866 to Brundrett et al.

U.S. Patent No. 6,950,932 to Lavian et al.

O'Connell et al, "JFS: A Secure Distributed File System for Network Computers"

Thompson et al, "Certificate-Based Access Control For Widely Distributed Resources"

Alliance for Telecommunications Industry Solutions, "ATIS TELECOM GLOSSARY 2000"

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

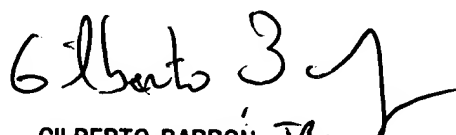
Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh  
Examiner  
Art Unit 2132

MD  
01/21/06

  
GILBERTO BARRON JR.  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100